



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/715,643	11/17/2000	Yoav Raz	EMS-00201	8061

26339 7590 06/28/2005

PATENT GROUP
CHOATE, HALL & STEWART
EXCHANGE PLACE, 53 STATE STREET
BOSTON, MA 02109

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/715,643

Applicant(s)

RAZ ET AL.

Examiner

Jung W. Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 April 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8, 13-16, 18-20, 22, 26-30, 36, 39-47, 49 and 50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☐ Claim(s) 1-8, 13-16, 18-20, 22, 26-30, 36, 39-47, 49 and 50 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 November 2000 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-8, 13-16, 18-20, 22, 26-30, 36, 39-47, 49 and 50 are pending.
2. Applicant amended claims 1, 22, 26, 36, 39 and 47 in the amendment filed on March 3, 2005 entered under 37 CFR 1.114.
3. Claims 9-12, 17, 21, 23-25, 31-35, 37 and 48 are canceled.
4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 3, 2005 has been entered.

Drawings

6. As specified in the previous office action, the drawings are objected to as being informal. The original drawings are acceptable for examination purposes but applicant will be required to submit formal drawings when a Notice of Allowance is submitted.

Response to Arguments

7. Applicant's arguments filed March 3, 2005 have been fully considered but they are not persuasive.

8. In response to applicant's arguments against the references individually (Remarks, pg. 18, 1st and 2nd paragraphs), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Wells discloses a method of detecting computer viruses on any given system from one or more files or one or more disk sectors (Wells, col. 2:54-63; claim 1). Frisch's disclosure suggest the benefits of a computing system as an aggregation of a plurality of filesystems, wherein a particular operating system exports its local filesystem to be mounted by a plurality of hosts. Frisch, pg. 395, fig. 9-1; pgs. 612-614 'Exporting Local Filesystems'. Kim's disclosure teaches a method and apparatus to monitor changes made to a filesystem using signatures, and a broad range of administrative options for nuanced monitoring capabilities. The combination of Wells and Frisch suggest a host having access to a file processed in connection with the virus detection. The combination of Wells and Kim suggest using fine grain monitoring techniques in connection with virus detection to enable, inter alia, scanning specific portions of the system (gathering, storing, and comparing information about computer system integrity is one of the key functions of the

Art Unit: 2132

invention of Wells [Wells, col. 1:51-52]). Hence, the limitations of the claimed invention are suggested or taught by the combined teachings of Wells, Frisch and Kim.

9. It is noted that the new limitation of the amended independent claims: "wherein the antivirus access one of the segments without using file-based information of any host having access to the segment" (claim 1), is taught by the prior art of record. The teaching of Wells modified by Frisch and Kim suggest an antivirus unit using the file-based information of a particular operating system it is scanning and not the file-based information of any host having access to the segment. A particular networked operating system using NFS to export its local filesystem mounted by hosts on their respective systems and running the anti-virus unit as taught by Wells on the particular networked operating system does not use the file-based information of any of the hosts to scan the local filesystem for viruses: all portions of the disk space on the particular operating system are accessed using the file-based information of the particular operating system. Wells, col. 9:1-4.

Claim Rejections - 35 USC § 103

10. Claims 1-8 and 13-16, 18-20, 22, 26-30, 36, 39-42, and 44-47, 49 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wells U.S. Patent No. 6,338,141 (hereinafter Wells) in view of Frisch Essential System Administration (hereinafter Frisch) and Kim "The Design and Implementation of Tripwire: A File System Integrity Checker" (hereinafter Kim).

11. As per claim 1, Wells discloses a method of detecting computer viruses on a single, stand-alone computer system or on a networked machine using an antivirus unit, wherein a user of the antivirus unit designates a set of files on a system to be scanned (see Wells, abstract; col. 9:1-4). Wells does not expressly disclose providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments. However, this configuration is found in networked operating systems. For example, Frisch teaches a UNIX operating system that enables a flexible partitioning capability wherein each partitioned segment is accessed using a different file system. Frisch, pgs. 409-414 'From Disks to Filesystems', especially pg. 409, first paragraph in the section. Moreover, Frisch discloses exporting local filesystems by a particular system for network access by other hosts to mount to their system. Frisch, pgs. 612-614 'Exporting Local Filesystems'. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the method of detecting a virus to be actuated on a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments, since it enables an administrator broader control to allow or restrict access to information on a disk by segmenting the disk on a partition level as taught by Frisch. Frisch, page 394, 2nd and 3rd paragraphs.

Art Unit: 2132

12. Further, Wells does not expressly disclose scanning for a virus on a portion of the disk that includes a part of the first and second segments. However, means of selectively checking the integrity of separate filesystems on a disk is a feature of the UNIX tool Tripwire. Kim teaches how different filesystems on a disk can be checked by entering the paths of relevant filesystems as well as corresponding selection-masks, which classifies how to observe changes in the filesystem, in the Tripwire configuration file. Kim, page 11, Figure 2 and related text. Furthermore, Kim teaches Tripwire as a function operating in a larger security methodology: the results of a Tripwire check can be used by a filter program. Kim, page 12, 2nd paragraph, 'quiet option'. It would be obvious to one of ordinary skill in the art at the time the invention was made to selectively scan separate filesystems on a disk space for viruses since it enables the method to secure any suspicious subset of data on a disk, even across partitioned boundaries.

13. Moreover, the invention of Wells scans all types of files and does not limit scanning to only non-native files (Wells, 2:15-20); also file sharing between different operation systems is a common feature among networked systems. As taught by Frisch in a different chapter, non-native files are transferred between a UNIX system and any reachable system (non-local and/or non-UNIX) using commands "ftp" and "telnet". Frisch, pg. 587, 4th and 5th bullets. Non-native files downloaded from non-local and/or non-UNIX platforms are incorporated into the local filesystem and likewise are a portion of the disk space to be scanned. It would be obvious to one of ordinary skill in the art at the time the invention was made for the antivirus unit, using a particular

Art Unit: 2132

operating system, to access non-native files created using operating systems different from the particular operating system that is used by the antivirus unit in connection with scanning at least parts of the disk space for viruses since file sharing is a common technique between different operating systems as known to one of ordinary skill in the art and as taught by Frisch. Ibid.

14. Finally, the invention of Wells modified by Frisch and Kim which runs on the particular operating system uses file based information of the particular operating system to access the segments, and not the file-based information of any host having access to the segment. The aforementioned cover the limitations of claim 1.

15. As per claim 2, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the first and second segments correspond to different physical portions of the disk space. Frisch, pg. 410, Figure 9-3. The aforementioned cover the limitations of claim 2.

16. As per claim 3, the rejection of claim 2 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments overlap. Frisch, pgs. 39-41, "Links". It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second segments to overlap to enable information pertinent to multiple segments to be shared between the segments as taught by Frisch. Ibid. The aforementioned cover the limitations of claim 3.

17. As per claim 4, the rejection of claim 2 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments do not overlap. Frisch, pg. 395, Figure 9-1, disk 1. It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second segments to not overlap to organize segments into distinct logical partitions as taught by Frisch. Ibid. The aforementioned cover the limitations of claim 4.

18. As per claim 5, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments correspond to logical entities. Frisch, pg. 395, Figure 9-1, disk 1. It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second segment to correspond to logical entities since it enables a direct correlation between a physical partition and a logical partition as taught by Frisch. Ibid. The aforementioned cover the limitations of claim 5.

19. As per claim 6, the rejection of claim 5 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments overlap. Frisch, pgs. 39-41, "Links". It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second segments to overlap to enable information pertinent to multiple segments to be shared

Art Unit: 2132

between the segments as taught by Frisch. Ibid. The aforementioned cover the limitations of claim 6.

20. As per claim 7, the rejection of claim 5 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments do not overlap. Frisch, page 395, Figure 9-1, disk 1. It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second segments to not overlap to organize segments into distinct logical partitions as taught by Frisch. Ibid. The aforementioned cover the limitations of claim 7.

21. As per claim 8, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the part of the disk space that is scanned by the antivirus unit corresponds to particular types of files stored in the disk space. Wells, col. 9, lines 1-4. The aforementioned cover the limitations of claim 8.

22. As per claim 13, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Kim teaches implementing at least part of Tripwire using stand-alone hardware. Kim, page 12, section 4.3.1. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement at least part of the antivirus unit using stand-alone hardware to ensure the inviolability of the integrity

Art Unit: 2132

database used by Tripwire. Kim, page 12, section 4.3.1, first paragraph in the section, 2nd sentence. The aforementioned cover the limitations of claim 13.

23. As per claim 14, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch and Kim teach implementing at least part of the antivirus unit as a process running on at least one of the hosts. Frisch, page 43, 'Processes'; Kim, page 10, section 4.1.2, 'Scalability' and section 4.1.3, 'Configurability and flexibility'; Wells, col. 3, lines 10-11. It would be obvious to one of ordinary skill in the art at the time the invention was made for a part of the antivirus unit be a process running on at least one of the hosts since any application run on a machine comprises at least one process on the machine: as defined by Frisch, a process is a single program running in its own virtual address space. Frisch, page 43, last paragraph, first sentence. The aforementioned cover the limitations of claim 14.

24. As per claim 15, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches the useable areas of a disk space are partitioned into separate segments in any given partitioned disk. Frisch, page 395, Figure 9-1, disk 1; page 410, Figure 9-3. It would be obvious to one of ordinary skill in the art at the time the invention was made for the useable areas of the disk space to be partitioned into separate segments to enable each disk partition to be usable to a user or application. The aforementioned cover the limitations of claim 15.

Art Unit: 2132

25. As per claim 16, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Wells and Kim teach the antivirus unit scans useable areas of the disk space. Kim, page 11, Figure 2; Wells, col. 1, lines 54-60. It would be obvious to one of ordinary skill in the art at the time the invention was made for the antivirus unit to scan useable areas of the disk space since these areas are workspaces having read/write privileges for users and applications and are prone to integrity attacks when a virus attains these privileges. The aforementioned cover the limitations of claim 16.

26. As per claim 18, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein a particular segment assigned to a first host is inaccessible to other hosts. Frisch, page 29, Table 2-3, 'no access'; page 30, 5th line 'Other Access' and Figure 2-1; pages 228-229 'Using Groups Effectively', especially page 228, 4th paragraph, second sentence. It would be obvious to one of ordinary skill in the art at the time the invention was made for a particular segment assigned to a first host to be inaccessible to other hosts for the purpose of enforcing non-use of those who do not require access to a segment. Frisch, page 228, 4th paragraph, second sentence. The aforementioned cover the limitations of claim 18.

27. As per claim 19, the rejection of claim 18 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein all

Art Unit: 2132

of the segments are at least readable by the antivirus unit. Frisch, page 29, Table 2-3, 'read access only'; page 30, 3rd line 'Group access' and Figure 2-1; pages 228-229 'Using Groups Effectively', especially page 228, 3rd paragraph, first sentence and 4th paragraph, last sentence. It would be obvious to one of ordinary skill in the art at the time the invention was made for all of the segments to be readable by the antivirus unit to enable the antivirus unit to comprehensively check the integrity of the disk. Frisch, page 228, 3rd paragraph, first sentence and 4th paragraph. The aforementioned cover the limitations of claim 19.

28. As per claim 20, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Kim and Frisch teach that at least a portion of the antivirus unit is provided on at least some controllers for disks corresponding to the disk space. Kim, page 11, Figure 2, first entry '/etc' and Section 4.2; Frisch, pages 398-405, 'The Filesystem Configuration File', especially page 398, '/etc/fstab'. It would be obvious to one of ordinary skill in the art at the time the invention was made for a portion of the antivirus unit to be provided on at least some controllers for disks corresponding to the disk space to enable a comprehensive integrity check methodology. The aforementioned cover the limitations of claim 20.

29. As per claim 22, the rejection of claims 1-8, 13-16 and 18-20 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Kim teaches a first scan at a first time and a second scan at a second time after the first time, wherein the results of the

Art Unit: 2132

first scan are taken into consideration in the performing of the second scan as outlined in the invention covered in the claim 1-8, 13-16 and 18-20 rejections. Kim, page 14, section 4.5. It would be obvious to one of ordinary skill in the art at the time the invention was made for there to be a first virus scan at a first time and a second virus scan at a second time after the first time and dependent on the results of the first scan since the scans are automated on a periodic basis and the integrity of the segments must be accounted for consistent with preceding scans starting with the inception of the checks to ensure integrity is maintained over the course of multiple periods. Kim, page 14, section 4.5, 1st paragraph of the section, 3rd sentence. The aforementioned cover the limitations of claims 22.

30. As per claims 26-30, they are apparatus claims corresponding to claims 1-8 and they do not teach or define above the information claimed in claims 1-8. Therefore, claims 26-35 are rejected as being unpatentable over Wells in view of Frisch and Kim for the same reasons set forth in the rejections of claims 1-8.

31. As per claim 36, it is an apparatus claim corresponding to claim 22 and it does not teach or define above the information claimed in claim 22. Therefore, claim 36 is rejected as being unpatentable over Wells in view of Frisch and Kim for the same reasons set forth in the rejection of claim 22.

32. As per claims 39, 42 and 44-46, they are apparatus claims corresponding to claims 1, 13, 14 and 20, and they do not teach or define above the information claimed in claims 1, 13, 14 and 20. Therefore, claims 39, 42 and 44-46 are rejected as being unpatentable over Wells in view of Frisch and Kim for the same reasons set forth in the rejections of claims 1, 13, 14 and 20.

33. As per claim 40, the rejection of claim 39 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Kim teaches an embodiment of Tripwire wherein the means for coupling includes means for coupling to only one storage device. Kim, pages 14-15, section 5. It would be obvious to one of ordinary skill in the art at the time the invention was made for the means for coupling to include means for coupling to only one storage device to provide a personal integrity checking means. Kim, page 14, section 5, 1st paragraph in the section. The aforementioned cover the limitations of claim 40.

34. As per claim 41, the rejection of claim 39 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Kim teaches an embodiment of Tripwire wherein the means for coupling includes means for coupling to more than one storage device. Kim, page 10, section 4.1.2, 'Scalability'. It would be obvious to one of ordinary skill in the art at the time the invention was made for the means for coupling to include means for coupling to more than one storage device to share one configuration of the integrity checker across a multitude of storage devices for a consistent integrity check

Art Unit: 2132

methodology across the storage network. Kim, page 10, section 4.1.2, 1st and 2nd paragraph in the section. The aforementioned cover the limitations of claim 41.

35. As per claims 47, 49 and 50, they are apparatus claims corresponding to claims 13, 20 and 22, and they do not teach or define above the information claimed in claims 13, 20 and 22. Therefore, claims 47, 49 and 50 are rejected as being unpatentable over Wells in view of Frisch and Kim for the same reasons set forth in the rejections of claims 13, 20 and 22.

36. Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wells in view of Frisch and Kim, and further in view of Tso et al. U.S. Patent No. 6,088,803 (hereinafter Tso).

37. As per claim 43, the rejection of claim 42 under 35 U.S.C. 103(a) is incorporated herein. (supra) Wells does not specify an embodiment wherein the antivirus unit is interposed between the at least one storage device and the at least one host. Tso discloses an antivirus accelerator for computer networks wherein an antivirus unit is interposed between a storage device and a host, wherein files requested by the host is first scanned by the antivirus unit then submitted to the host if no virus is detected. Tso, figure 1 and related text. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the apparatus of Tso to the apparatus of Wells. Motivation for such a combination safeguards information being transferred from a

Art Unit: 2132

storage unit to a host. Tso, col. 1, lines 48-55. The aforementioned cover the limitations of claim 43.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jk
June 23, 2005

Jung W Kim
Examiner
Art Unit 2132



GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100